

3700 Bay Area Boulevard
Houston, Texas 77058-1199

NAS9-18874

Advanced Avionics Technology Lab

1993 Accomplishments

(NASA-CR-188274) ADVANCED AVIONICS
TECHNOLOGY LAB 1993 ACCOMPLISHMENTS
Final Report (IBM) 36 p

N94-71802

Unclassified

29/06 0003791

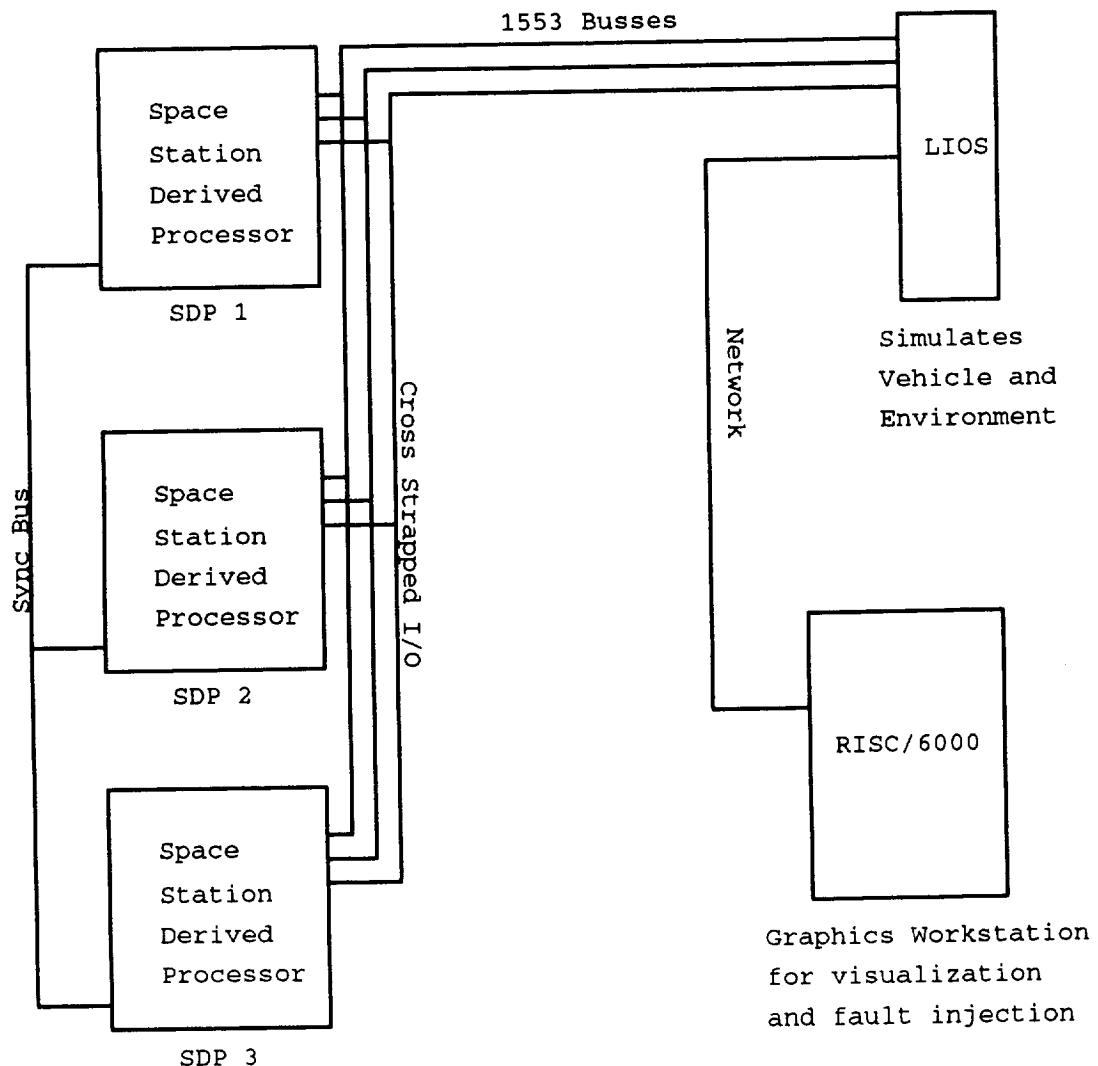
Rich Petras
Ted Smith
September 30, 1993



AATL 1993 Accomplishments

Assembled AATL

The Advanced Avionics Technology Lab (AATL) was assembled in a Triple Modular Redundant (TMR) configuration. See Figure below.





Ported Avionics Application from VM 370

Avionics Applications developed in Ada for the VM370 host system were ported to the 80386 platform. The avionics were divided into the control application and the environment simulation. The control application runs in the TMR processors. The environment and vehicle simulation runs in a 80486 based PS/2 processor.

Developed Graphics Output and Controls for RISC/6000

A RISC/6000 processor was networked to the AATL simulation processor to act as a control interface for the simulation. A graphical display was developed to allow visualization of the vehicle attitude. X-windows control panels were developed to allow fault injection and control of the simulation.

Developed Ada Sync Package

An Ada software package was developed to interface to the sync hardware in the TMR processors. It provides software sync points and redundant set formation procedures for the control application.

Fail To Sync Processing

Within the control application, procedures for handling a fail to sync condition were developed. Methods for determining the failed processor were used to remove the processor from the redundant set.

Redundant Set Reformation

When a failed processor was restored, a procedure was developed to allow the processor back into the redundant set.

RCS Fault Injection

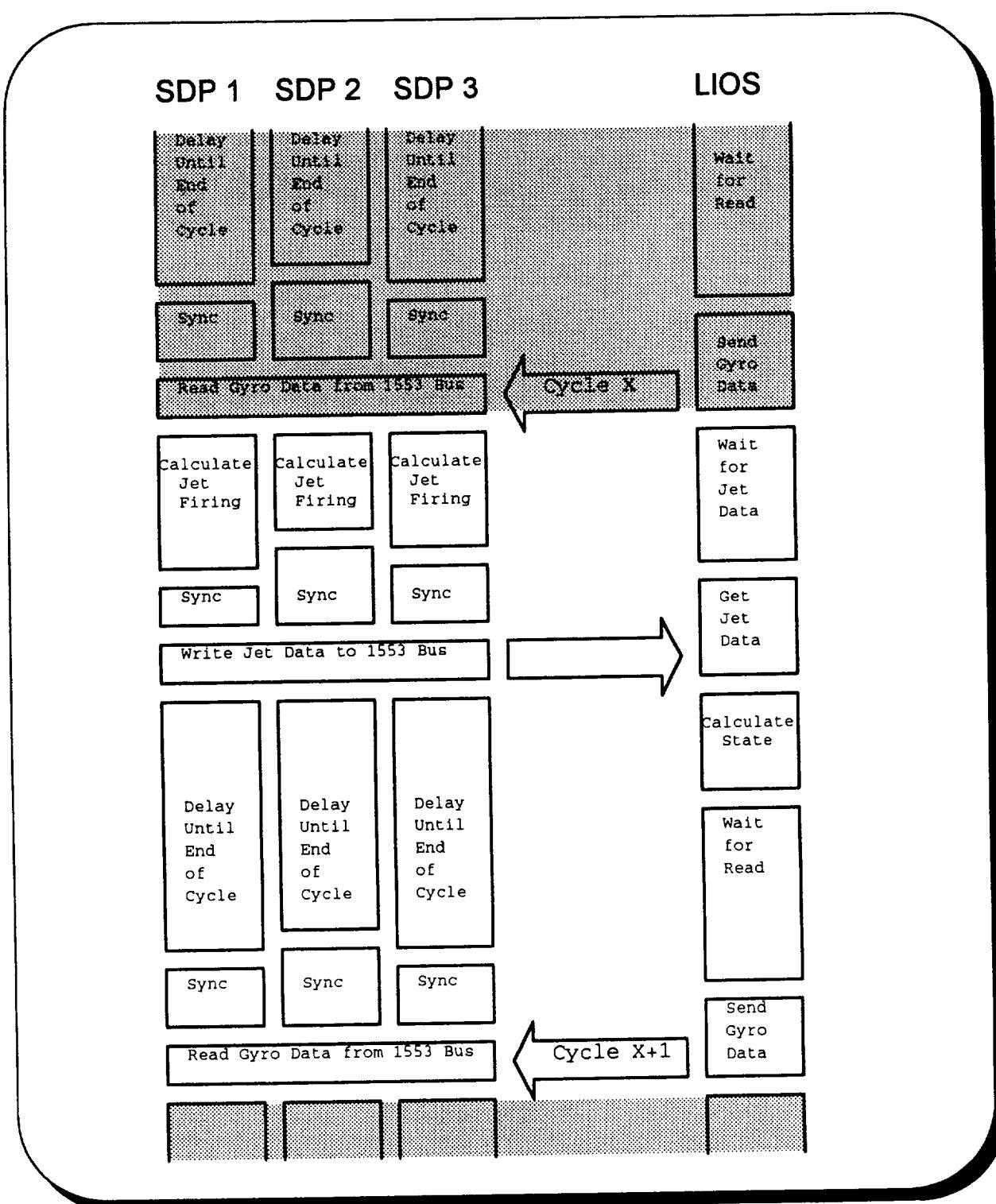
In the simulation processor, we developed procedures to inject faults into the vehicle simulation. A control panel on the RISC/6000 workstation was used to fail Reaction Control System jets on or off. A similar method will be used to inject other types of faults.

Use Microsecond Timer for Time Management

The timer available from Ada had a 0.1 second resolution. This was unacceptable for real time performance. We wrote procedures to use the microsecond timer available on the TMR processors from within an Ada program.



SOFTWARE SYNC PROCESS





**FAULT TOLERANT
AVIONICS ARCHITECTURE
ANALYSIS
(TMR VS P-O-P)**

**TED SMITH
IBM FSC**

JUNE 30, 1993

CONTRACT : NASS-18874

ACRONYM & ABBREVIATION LIST

ACCM	ACCELEROMETER
ARCH	ARCHITECTURE
ATT DET	ATTITUDE DETERMINATION
C&T	COMMUNICATION AND TRACKING
D/A	DIGITAL TO ANALOG CONVERSION
EHA	ELECTROHYDRAULIC ACTUATOR
EMA	ELECTROMECHANICAL ACTUATOR
FCC	FLIGHT CONTROL COMPUTER
FCR	FAULT CONTAINMENT REGION
FDIR	FAULT DETECTION, ISOLATION & RECOVERY
FMEA	FAILURE MODES & EFFECTS ANALYSIS
FT	FAULT TOLERANT
GNC	GUIDANCE, NAVIGATION AND CONTROL
IMU	INERTIAL MEASUREMENT UNIT
LCC	LIFE-CYCLE COST
LRU	LINE REPLACEABLE UNIT
MDM	MULTIPLEXER / DEMULTIPLEXER
MSEC	MILLISECOND
NAV	NAVIGATION
NMR	N - MODULAR REDUNDANCY
NOS	NETWORK OPERATING SYSTEM
P-O-P	PAIR-OF-PAIR
P/S	POWER SUPPLY
QMR	QUAD MODULAR REDUNDANCY
RIU	REMOTE INTERFACE UNIT
RLG	RING LASER GYRO
RM	REDUNDANCY MANAGEMENT
SPF	SINGLE POINT FAILURE
SRU	SHOP REPLACEABLE UNIT
SW	SOFTWARE
SYNCH	SYNCHRONIZATION (OR SYNCHRONIZE)
TMR	TRIPLE MODULAR REDUNDANCY
TSP	TWISTED SHIELDED PAIR
TV	THRUST VECTOR CONTROL

PRELIMINARY CONCLUSIONS

- THERE ARE ARGUMENTS FOR BOTH TMR & P-O-P
- THESE ARGUMENTS INVOLVE:
 - COST (FMEA, RECOVERY SOFTWARE)
 - TESTABILITY
 - SCALEABILITY TO 2-FT
 - PACKAGING
 - FEDERATED ARCHITECTURE SUPPORT
- THERE ARE AREAS WHERE TMR & P-O-P ARE COMPARABLE
- THESE AREAS INVOLVE:
 - FAULT LATENCY
 - RELIABILITY
 - MAINTAINABILITY
 - POWER/WEIGHT/VOLUME
 - RISK

ANALYSIS RESULTS

ARGUMENTS FOR TMR

TMR ADVANTAGE	P-O-P DISADVANTAGE
COST	<ul style="list-style-type: none"> * FMEA - SIMPLIFIED * NO SWITCHOVER SOFTWARE
TESTABILITY	<ul style="list-style-type: none"> * SIMPLE FAULT INJECTION
SCALABILITY	<ul style="list-style-type: none"> * INHERENT IN NMR ARCH
PACKAGING	<ul style="list-style-type: none"> * 3 PHYSICALLY SEPARATE BOXES * GIVES ADDED FAULT PROTECTION
	<ul style="list-style-type: none"> * FMEA - COMPLEX * FAIL-OVER SOFTWARE DEVELOPMENT
	<ul style="list-style-type: none"> * COMPLEX MICRO-LEVEL FD/R
	<ul style="list-style-type: none"> * REDESIGN OR ACCEPT 1-FT REGIONS
	<ul style="list-style-type: none"> * VULNERABILITY OF ONE BOX

ANALYSIS RESULTS ARGUMENTS FOR P-O-P

	P-O-P ADVANTAGE	TMR DISADVANTAGE
FEDERATED ARCH	<ul style="list-style-type: none">* SUPPORTS DSTR PROC BETTER AND MULTI-ACCESS NETWORKING* P-O-P USED IN IMU & RIU	<ul style="list-style-type: none">* BEST IMPLEMENTED WITH PT-TO-PT BUS (MIL-STD-1553)* TMR COSTLY FOR IMU

ANALYSIS RESULTS (AREAS WITH NO CLEAR WINNER)

TMR CHARACTERISTIC	P-O-P CHARACTERISTIC
FAULT LATENCY	<ul style="list-style-type: none"> * ZERO (UN-INTERRUPTED CONTROL) * COMMAND STRING VOTING
RELIABILITY	<ul style="list-style-type: none"> * INSIGNIFICANTLY LOWER * STRING COUPLING * NO DYNAMIC RESTRINGING
MAINTAINABILITY	<ul style="list-style-type: none"> * ADEQUATE FOR LRU/SRU
PWR/WTIVOL	<ul style="list-style-type: none"> * 3 PROCESSOR BOARDS
RISK	<ul style="list-style-type: none"> * SHUTTLE NMR EXPERIENCE * BOEING, GD, IBM IR&D INVESTMENT * DELTA UPGRADE

ANALYSIS BASIS

COMMON ARCHITECTURE EVALUATION BASE

ITEM	BASIS
VEHICLE	<ul style="list-style-type: none"> * EXPENDABLE LAUNCH VEHICLE (ELV) * MANNED AND UNMANNED
ARCHITECTURE	<ul style="list-style-type: none"> * FEDERATED - FLIGHT CONTROL COMPUTER (FCC) <ul style="list-style-type: none"> - REMOTE I/F UNIT (RIU) - FAULT TOLERANT IMU
FAULT TOLERANCE	<ul style="list-style-type: none"> * MANNED - FO/FO/FS * UNMANNED - FO
AVIONICS RELIABILITY	<ul style="list-style-type: none"> * MANNED > 0.9999 * UNMANNED > 0.995
AVIONICS AVAILABILITY	<ul style="list-style-type: none"> * NO LAUNCH WITH FAULTS * UNAVAILABILITY AT PAD < 0.01
Maintenance (ON-LINE)	<ul style="list-style-type: none"> * FAULT ISOLATION TO LRU (BOX)
Maintenance (SHOP)	<ul style="list-style-type: none"> * FAULT ISOLATION TO SRU (CARD)

EVALUATION CRITERIA

ITEM	SPECIFICATION
FAULT LATENCY	* TIME TO CRITICALITY < 10 MILLISECONDS
RELIABILITY	* MANNED > 0.999 * UNMANNED > 0.99
AVAILABILITY	* UNAVAILABILITY AT PAD < 0.01
COST	* MINIMIZE : RECURRING / NON-RECURRING / LCC
PHYSICAL CHARACTERISTICS	* MINIMIZE : POWER / WEIGHT / VOLUME

TRADE ISSUES

ITEM	ISSUE
ARCHITECTURE	<ul style="list-style-type: none"> * SCALABILITY - SINGLE AND DUAL FT VERSIONS * FCRs - MACRO (STRINGS) VS MICRO (BOARD FCRs) * REDUNDANCY MANAGEMENT FOR SEQUENTIAL FAULTS
PACKAGING	<ul style="list-style-type: none"> * BACKPLANE BUS COMPLEXITY * POWER SUPPLIES & POWER DISTRIBUTION & CLOCKS
SINGLE POINTS OF FAILURE	<ul style="list-style-type: none"> * SWITCH-OVER LOGIC * SYNCHRONIZATION * I/O CROSS-STRAPPING
RELIABILITY	<ul style="list-style-type: none"> * PARTS COUNT
MAINTAINABILITY	<ul style="list-style-type: none"> * ON-LINE REPAIR FOR LAUNCH AVAILABILITY * COMPLEXITY OF LRU (IF BOX LEVEL) * ACCESSIBILITY AND RETEST SUPPORT (IF BOARD LEVEL)
COST	<ul style="list-style-type: none"> * DESIGN COMPLEXITY FOR DETECTION IN FCRs * DESIGN ANALYSIS (FMEA, ...) * NON-RECURRING (BACKPLANE COMPLEXITY, ...) * RECURRING (NUMBER COMPUTER BOARDS, ...) * SOFTWARE (RECOVERY, SYNCN, ...)

1 - FAULT TOLERANT COMPARISON

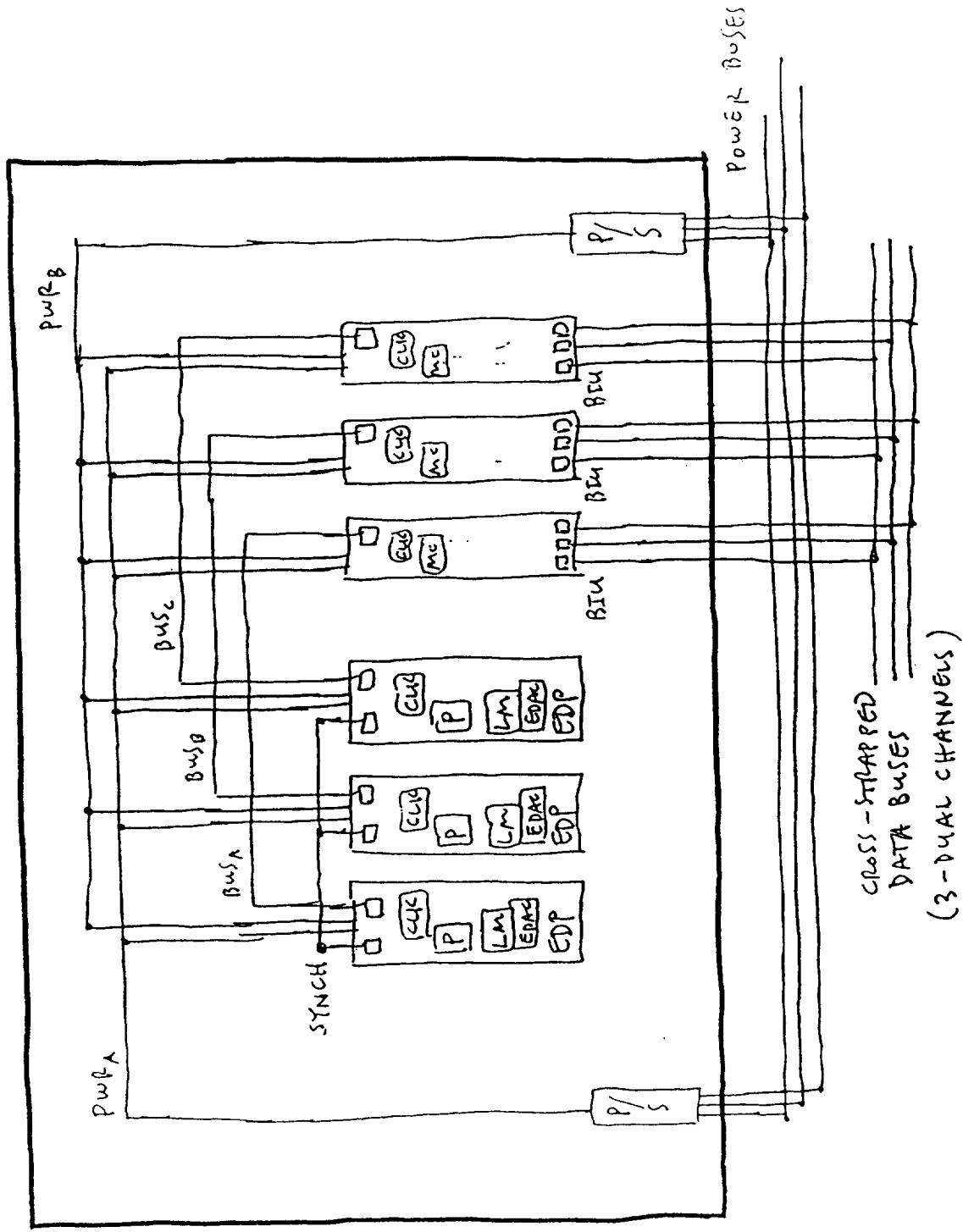
(TMR VS PAIR-OFF-PAIR)

FEATURE	TMR CHARACTERISTIC	P-O-P CHARACTERISTIC
ARCHITECTURE	<ul style="list-style-type: none"> * COMMAND STRINGS * PROCESSOR SYNCH * I/O CROSS-STRAP * TRIPLE REDUNDANCY WITH NO FDIR 	<ul style="list-style-type: none"> * MULTIPLE FAULT CONTAINMENT REGIONS (FCRs) - 8 IN FCC * DUAL REDUNDANCY WITH LOW LEVEL ERROR DETECTION/RETRY/FAIL-OVER
DETECTION	<ul style="list-style-type: none"> * NOT NECESSARY FOR SINGLE FAULT TOLERANCE 	<ul style="list-style-type: none"> * DIFFERENT SCHEMES PER FCR * P-O-P LOCK-STEP COMPARE * WATCHDOG TIMERS * BUS PARITY * COMMUNICATION PROTOCOL CHECKS * APPLICATION SUMCHECK
ISOLATION	<ul style="list-style-type: none"> * FORCE VOTE AT ACTUATOR FOR ENTIRE COMMAND STRING 	<ul style="list-style-type: none"> * FORCE VOTE AT ACTUATOR FOR TRIPLE D/A CHANNEL OUTPUT * FCR FAULT PROPAGATION BLOCKED BY DETECTION/RETRY MECHANISMS
RECOVERY	<ul style="list-style-type: none"> * NOT NECESSARY FOR SINGLE FAULT TOLERANCE 	<ul style="list-style-type: none"> * FAIL-OVER LOGIC IN EACH FCR (EXCEPT TRIPLE D/A OUTPUT CHANNELS)

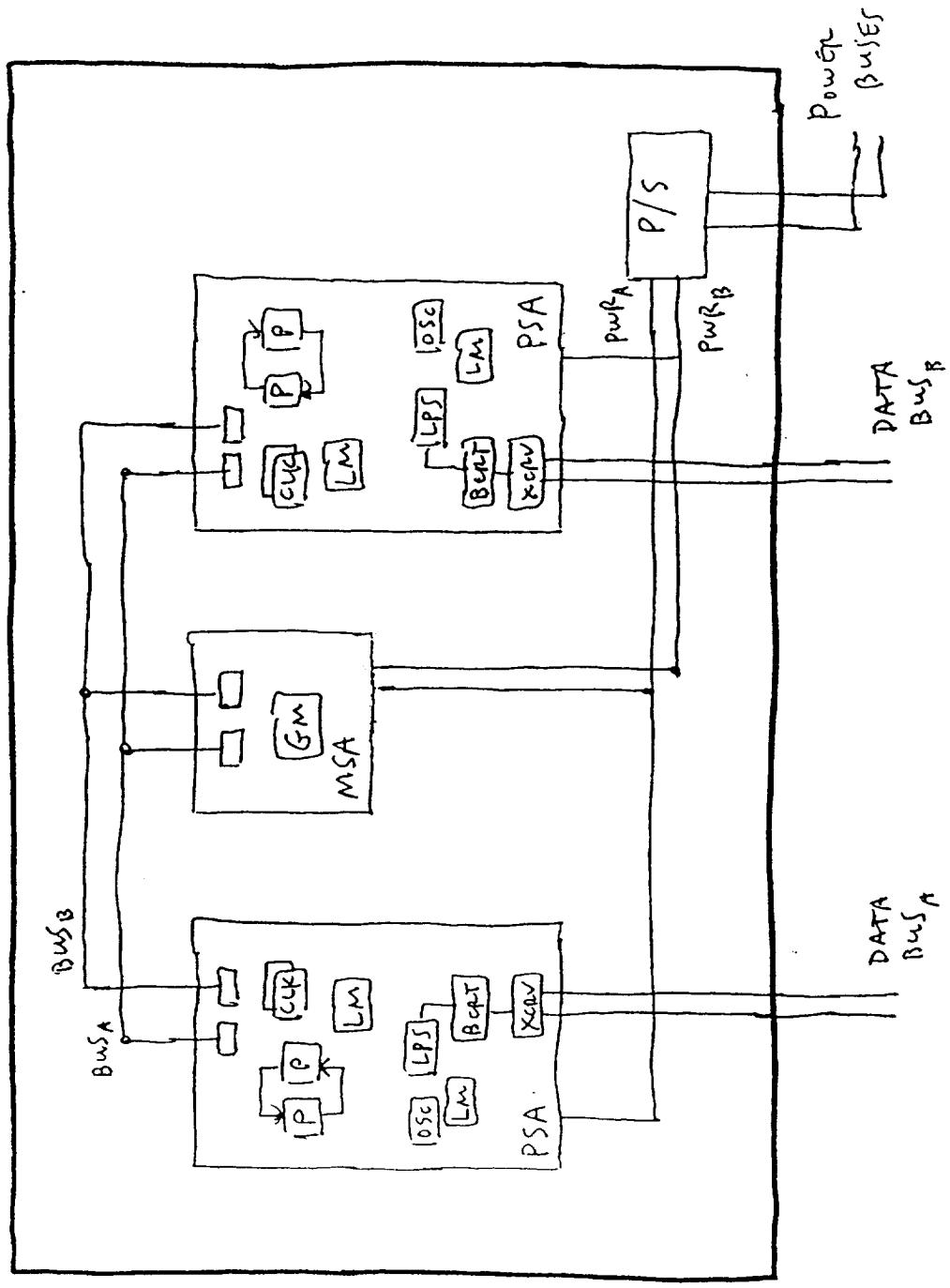
2 - FAULT TOLERANT COMPARISON (QMR VS TRIPLE-PAIRS)

FEATURE	QMR CHARACTERISTIC	P-O-P CHARACTERISTIC
ARCHITECTURE	<ul style="list-style-type: none"> * COMMAND STRINGS * PROCESSOR SYNCH * I/O CROSS-STRAP * QUAD REDUNDANCY WITH FD/R 	<ul style="list-style-type: none"> * MULTIPLE FAULT CONTAINMENT REGIONS (FCRS) * TRIPLE REDUNDANT PROCESSOR PLUS SOME DUAL REDUNDANCY * ACCEPTANCE OF SINGLE FAULT TOLERANCE IN HIGH REL COMPONENTS (P/S, BACKPLANE, ...)
DETECTION	<ul style="list-style-type: none"> * FAIL-TO-SYNCH * SUM WORD EXCHANGE 	<ul style="list-style-type: none"> * DIFFERENT SCHEMES PER FCR * P-O-P LOCK-STEP COMPARE * WATCHDOG TIMERS * BUS PARITY * COMMUNICATION PROTOCOL CHECKS * APPLICATION SUMCHECK
ISOLATION	<ul style="list-style-type: none"> * FORCE VOTE AT ACTUATOR FOR ENTIRE COMMAND STRING 	<ul style="list-style-type: none"> * FORCE VOTE AT ACTUATOR FOR QUAD D/A CHANNEL OUTPUT * FCR FAULT PROPAGATION BLOCKED BY DETECTION/RETRY MECHANISMS
RECOVERY	<ul style="list-style-type: none"> * REDUNDANCY MGT SW FOR SEQUENTIAL FAULTS * NO DYNAMIC RE-STRINGING 	<ul style="list-style-type: none"> * FAIL-OVER LOGIC IN EACH FCR (EXCEPT QUAD D/A OUTPUT CHANNELS)

TMR FLIGHT CONTROL COMPUTER

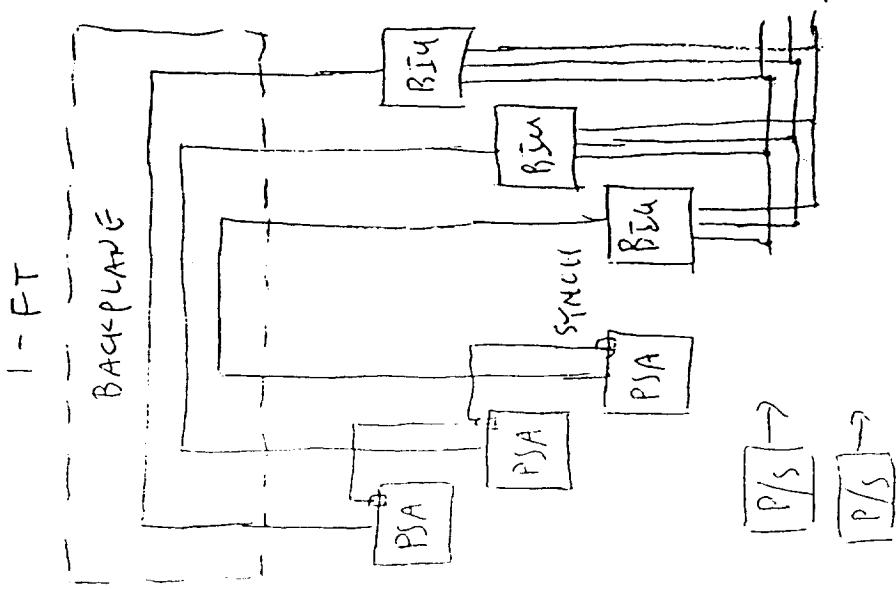


P-O-P
FLIGHT CONTROL COMPUTER



SCALEABILITY

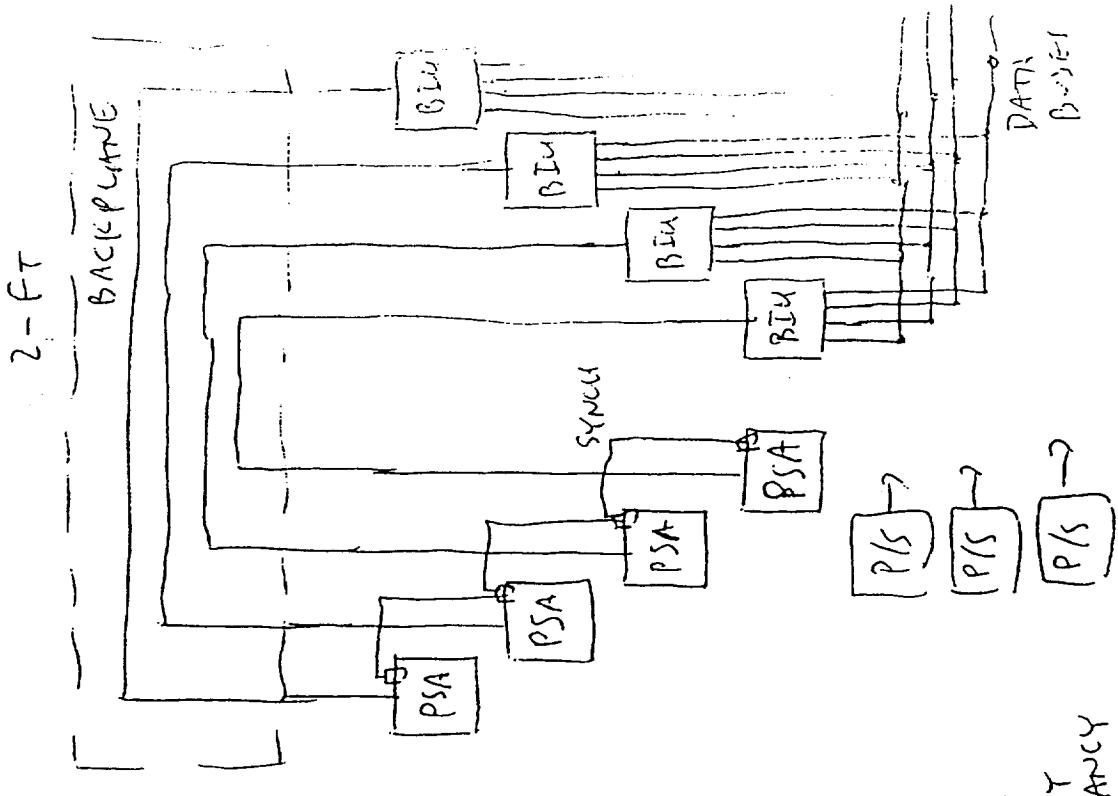
TMR SCALEABILITY



$\boxed{P/S} \rightarrow$
 $\boxed{\overline{P/S}} \rightarrow$

ISSUES:

- BACKPLANE COMPLEXITY
- P/S REDUNDANCY



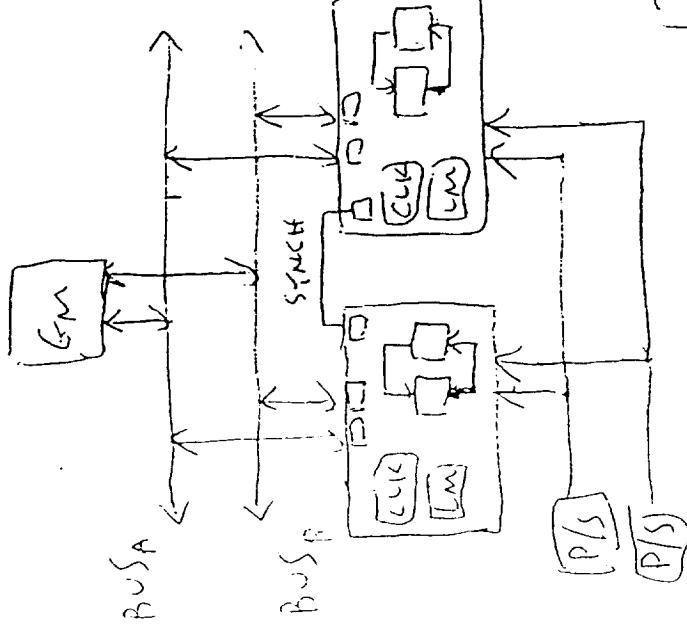
DATA
buses

$\boxed{P/S} \rightarrow$
 $\boxed{P/S} \rightarrow$
 $\boxed{P/S} \rightarrow$

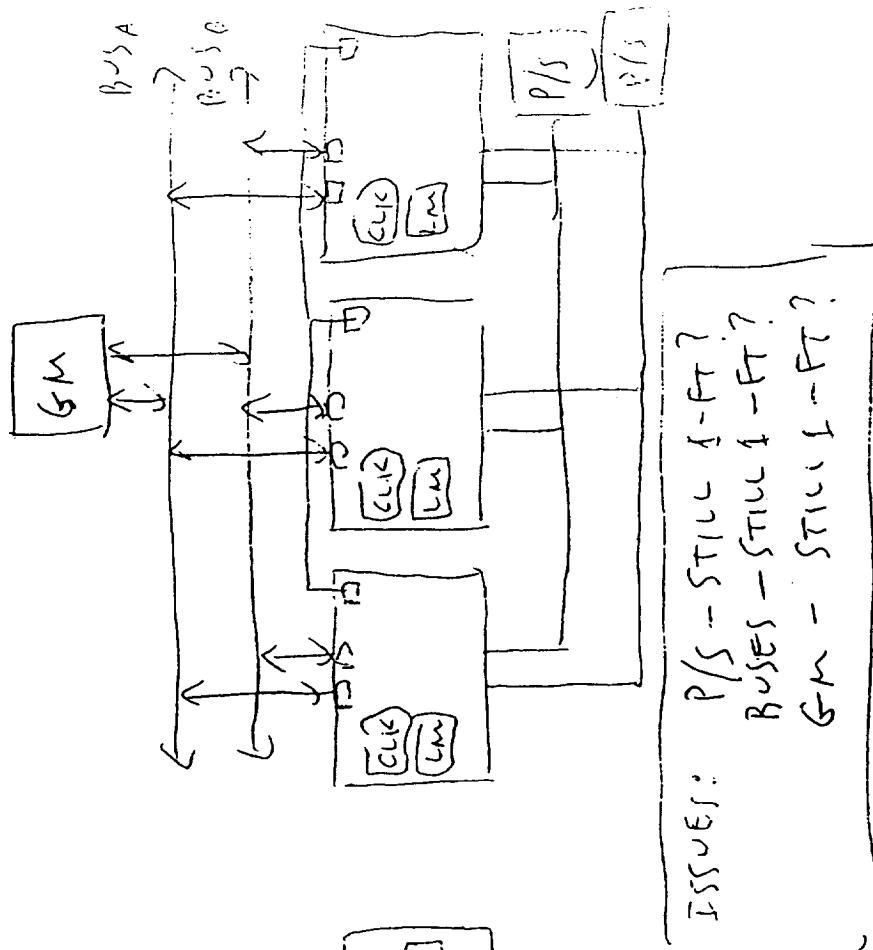
DATA
buses

P-O-P SCALEABILITY

1 - FT

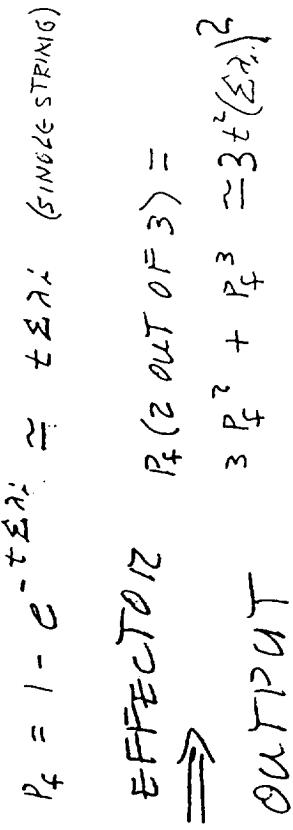
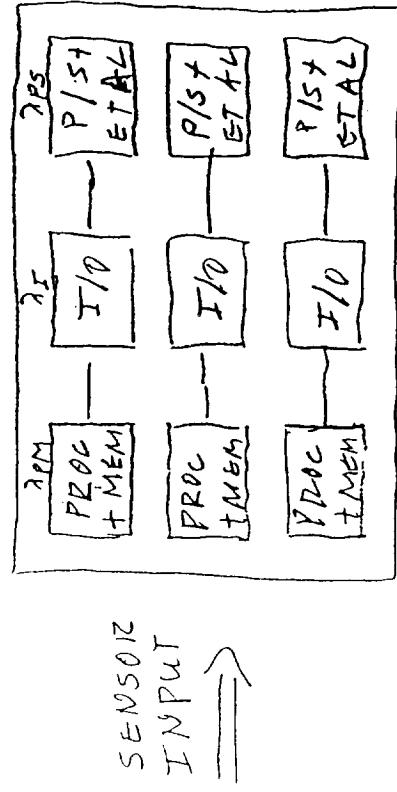


2 - FT



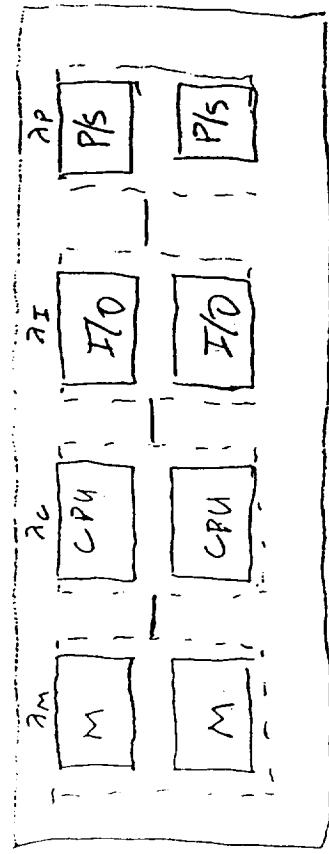
RELIABILITY ANALYSIS

TMR VS P-O-P RELIABILITY



TMR

$$P_{f_m} \approx (t \lambda_m)^2 \quad P_{f_c} \approx (t \lambda_c)^2 \quad P_{f_p} \approx (t \lambda_p)^2 \quad P_f = t^2 (\sum \lambda_i)^2$$



P O P

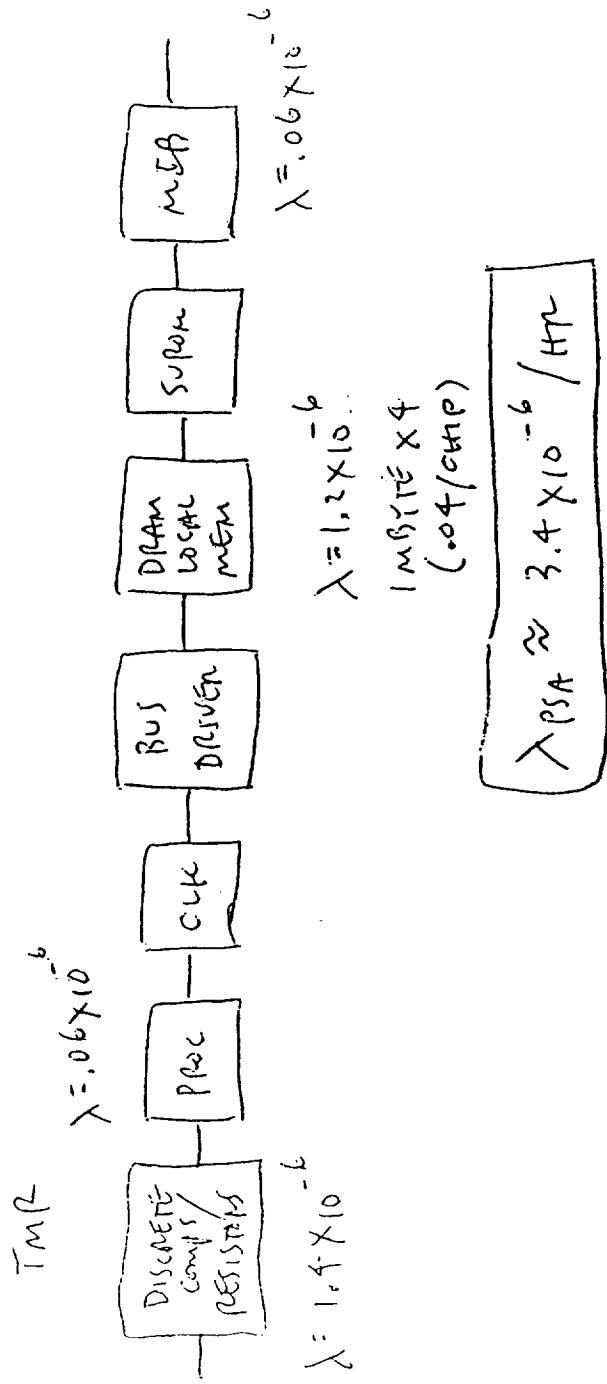
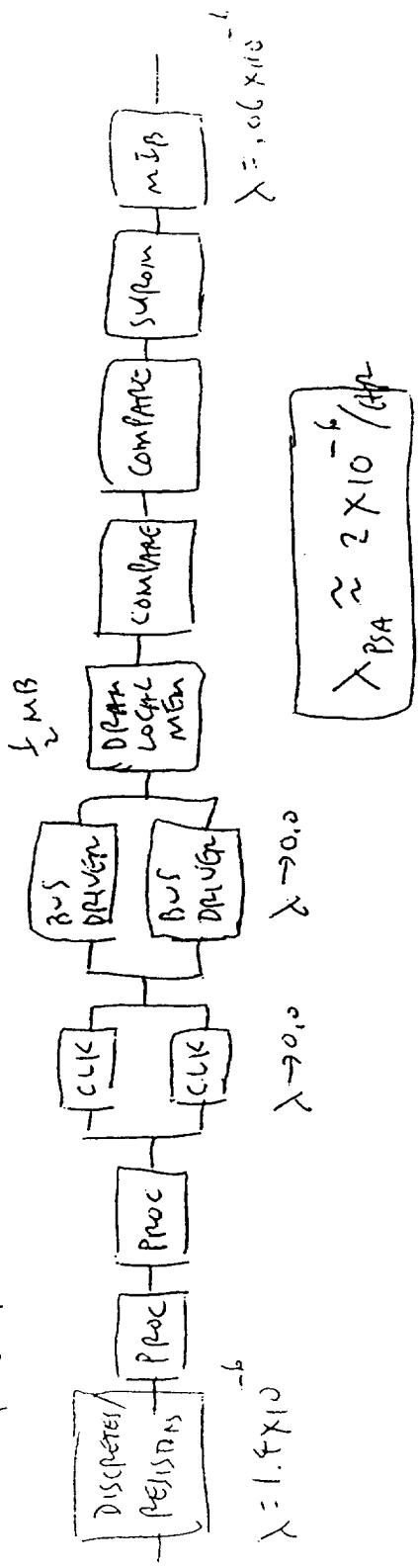
SSF Component	
EDP16	4×10^{-6}
BIU	3×10^{-6}
P/S + BACKUP	4.4×10^{-6}
MEM	1.2×10^{-6}

Pf (1HR MISSION)	
TMR	39.0×10^{-12}
POP	44.4×10^{-12}

PROCESSOR SUBASSEMBLY (PSA)

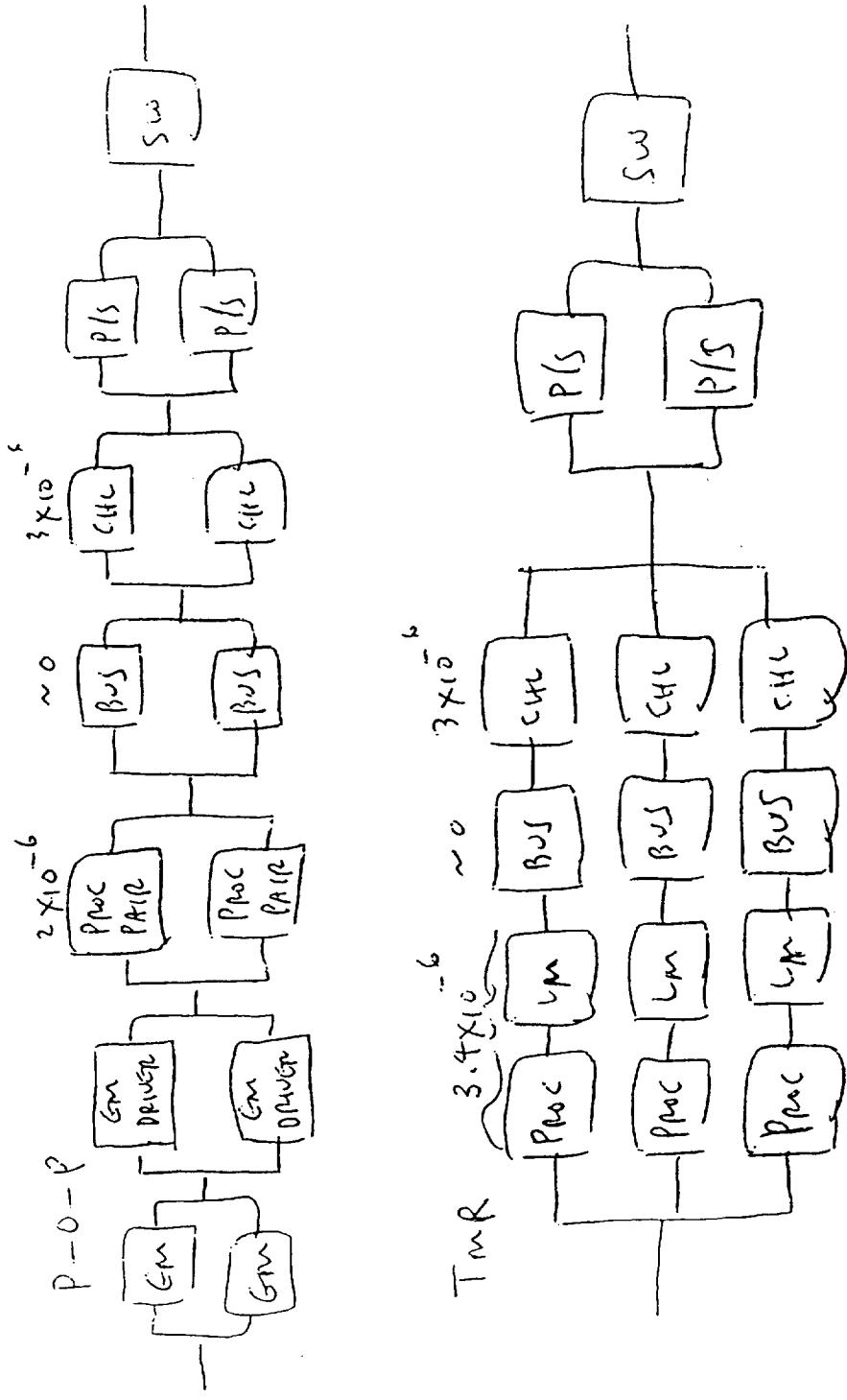
RELIABILITY ANALYSIS

$$P = 0 - P$$



FLIGHT CONTROL COMPUTER (FCC)

RELIABILITY ANALYSIS



REMAINING TMR VS P-O-P ANALYSIS ISSUES

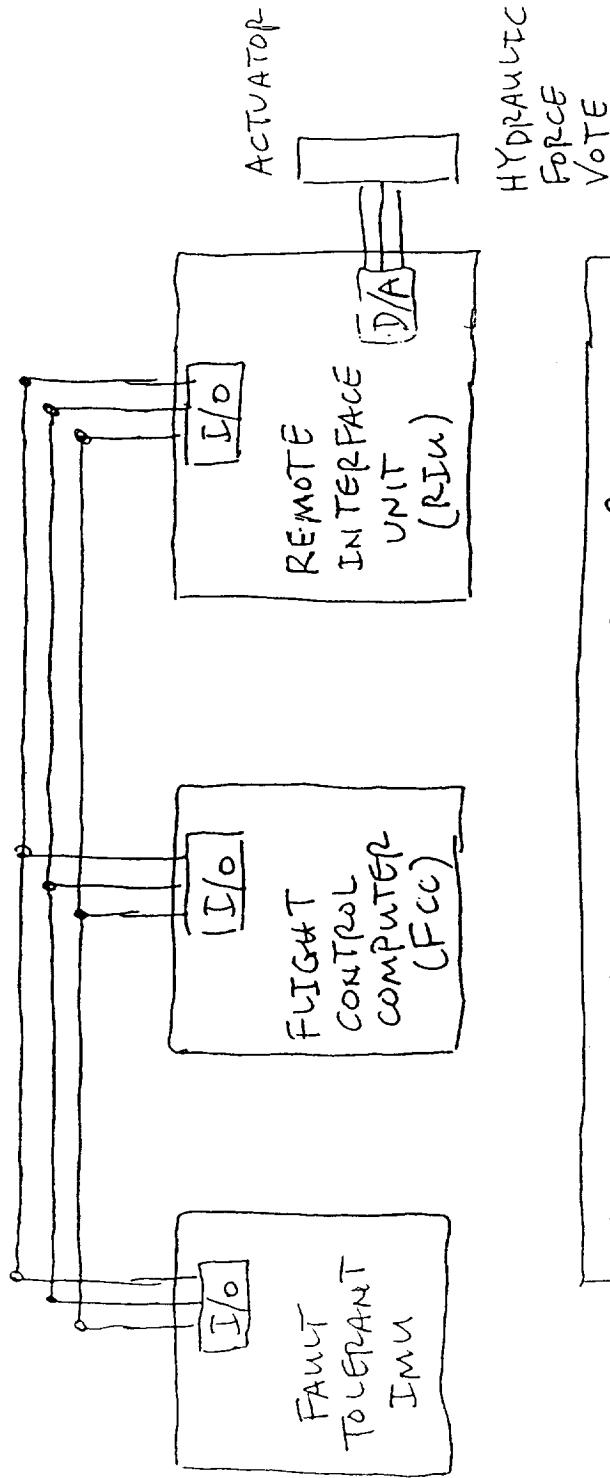
- *P-O-P*
 - ARE THERE SINGLE FAULTS THAT RESULT IN MULTIPLE ERRORS THAT CAN GO UNDETECTED OR DETECTABLE BUT UNRECOVERABLE? (I.E. BUS PARITY OR GLOBAL MEMORY)
 - DOES ADDED POP DETECTION & SWITCHOVER LOGIC REDUCE RELIABILITY SIGNIFICANTLY?
 - DO WE NEED SEPARATE MEMORY BOARD IN P-O-P ARCH? OR IS LOCAL MEMORY ON PROCESSOR PAGE SUFFICIENT? (REAL ESTATE LOSS FOR TWO PROCESSOR CHIPS AND DETECTION LOGIC)
 - WHEN WE SCALE P-O-P UP TO 2-FT DO WE NEED TWO MEMORY BOARDS?
 - SYNCH BETWEEN P-O-P ON BUS OR SYNCH LINES IN BACKPLANE OR SEMAPHORES IN GLOBAL MEMORY?
- *TMR*
 - TMR PACKAGING IN 1-BOX OR 3-BOXES?
 - BACKPLANE REDESIGN FOR 1-BOX QMR OR BUILT-IN SCALABILITY?
 - LIMIT ON SYSTEM BUSES IN BACKPLANE?
- *BOTH TMR & P-O-P*
 - CAN WE BACK OFF OF 2-FT FOR MANNED SYSTEMS WITH HIGH RELIABILITY?
 - STAY WITH DUAL PSS FOR 2-FT? (IF TMR IN 1-BOX) OR 3 POWER BUSES?
 - BUILT-IN SUPPORT FOR RETEST & CHECKOUT FOR REPAIR AT PAD?
 - ACCESSIBILITY FOR BOX OR BOARD ON-LINE REPAIR?

REMAINING AVIONICS ARCHITECTURE ISSUES

- **FEDERATED DISTRIBUTION**
 - IMU & RIU PACKAGING TO SUPPORT TMR FCCs?
 - SHOULD IMU RM BE DONE IN IMU OR FCC?
 - NON-GNC FUNCTION ALLOCATION TO FCC & RIU?
- **NETWORK**
 - MULTI-ACCESS NETWORK VERSUS POINT-TO-POINT BUSES?
 - PROTOCOL & NOS (EXPENSE & COMPLEXITY & DELAY VARIATIONS)?
 - MEDIA (TSP FOR INTERNAL COMM & FIBER FOR LAUNCH DATA BUS)?
- **AVIONICS INTERFACES**
 - C&T?
 - LAUNCH DATA BUSS?

COMMON TMR & P-O-P ARCHITECTURE FEATURES

DATA BUSSES (MIL-STD - 1553)



- FEDERATED ARCHITECTURE - IMU, FCC, RIU
- COMMUNICATION BUS - MIL-STD - 1553
- TVC ACTUATOR - HYDRAULIC FORCE VOTE
- PACKAGING - SINGLE BOX IMU, FCC, RIU

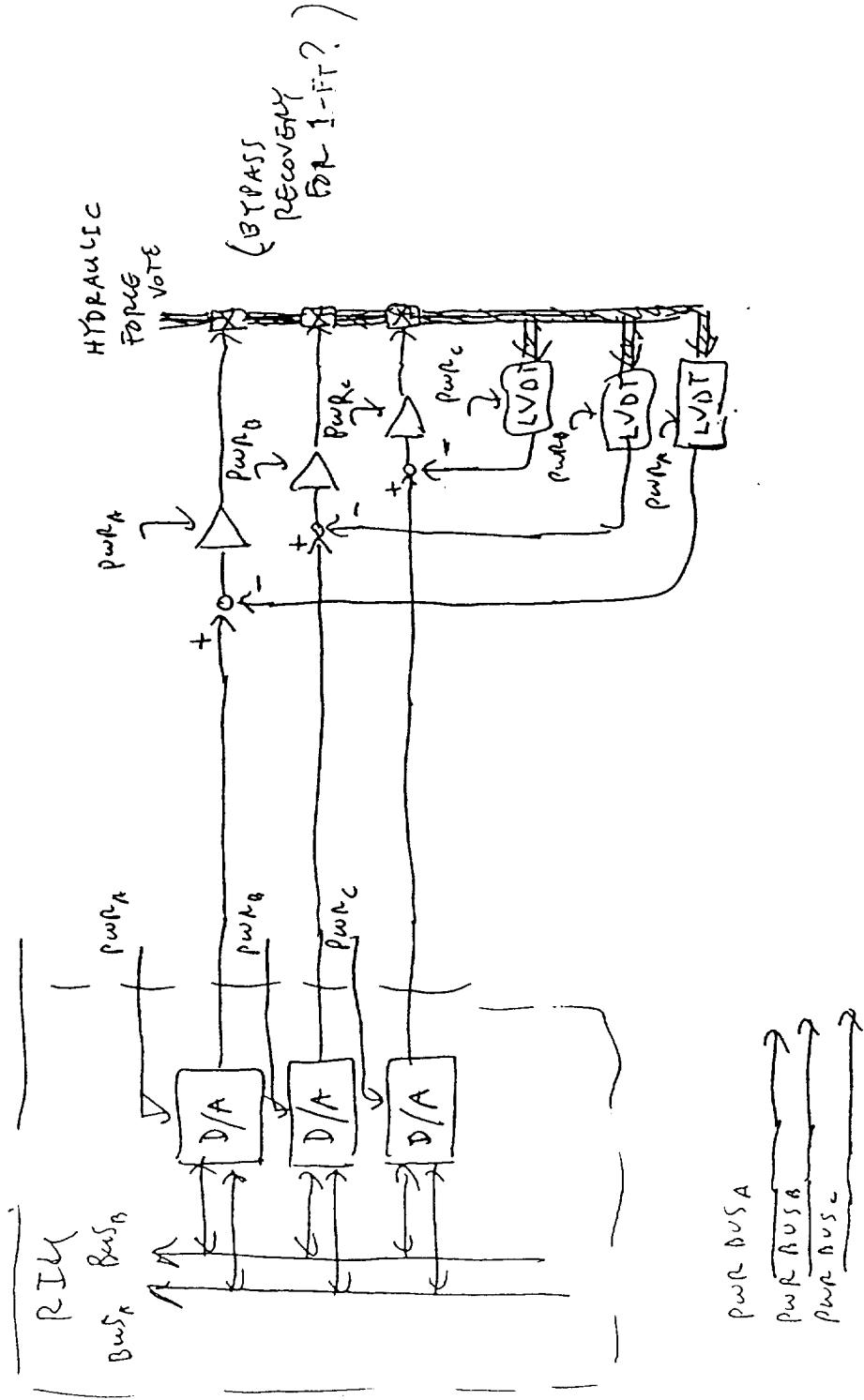
BACKUP MATERIAL

P-O-P FMEA

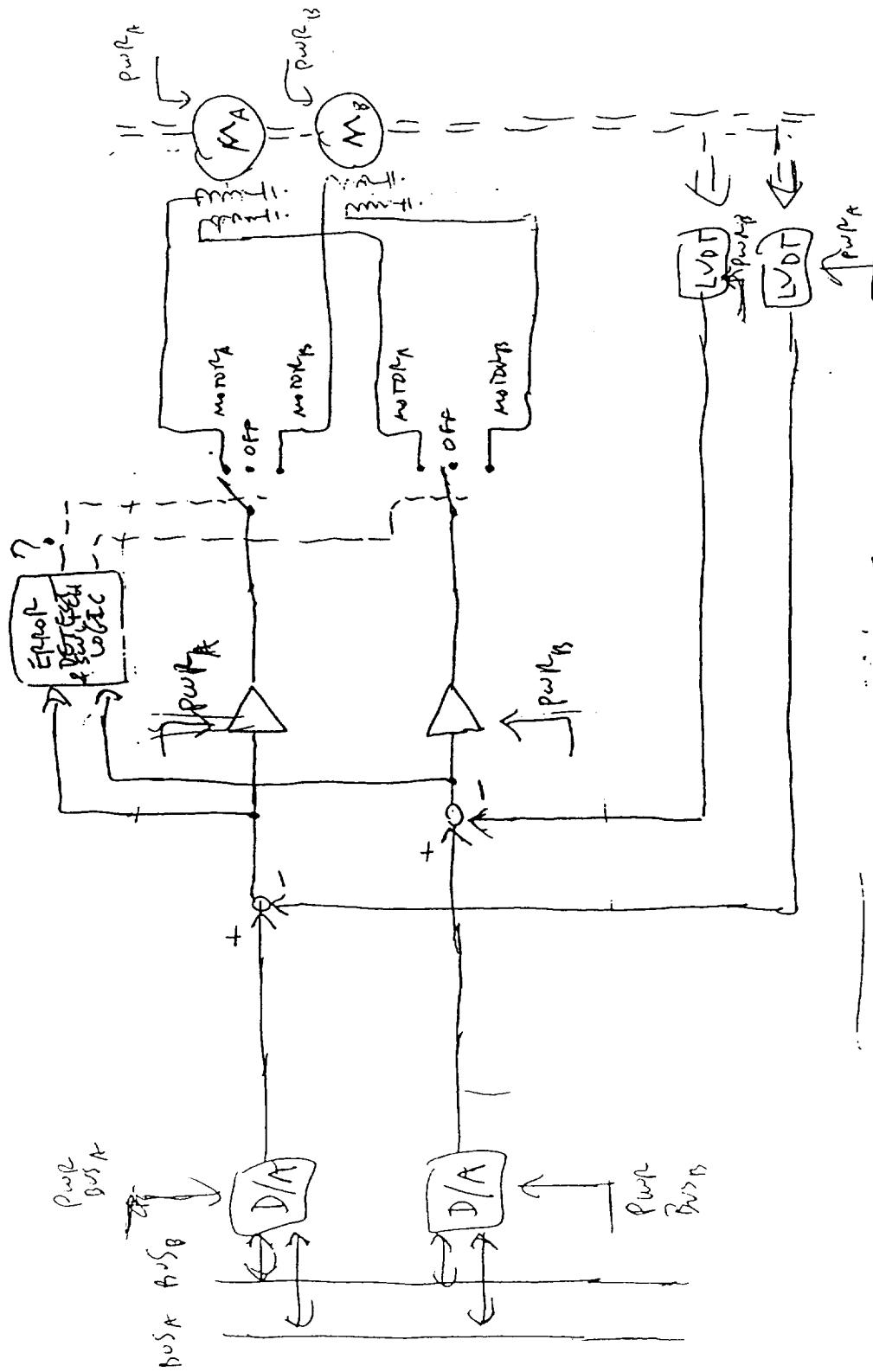
- **GLOBAL MEMORY**
 - CORRELATED ERRORS FROM SINGLE FAULT?
 - ARE 2-PICKED BITS CONSIDERED 2 FAULTS? (DETECTED BUT NOT CORRECTED)
- **COMPARATORS**
- **SWITCHOVER LOGIC**
 - FAULTS THAT LEAVE BOTH PAIRS DRIVING BUSES?
 - FAULTS THAT LEAVE NEITHER PAIR DRIVING BUSES?
 - SWITCHOVER TIME DELAY ACROSS FAULT SET? (RETRY TIME)
- **BUSES**
 - CORRELATED ERRORS FROM SINGLE FAULT?

TVC ACTUATOR INTERFACE

ACTUATOR FCRs (FORCE VOTE)



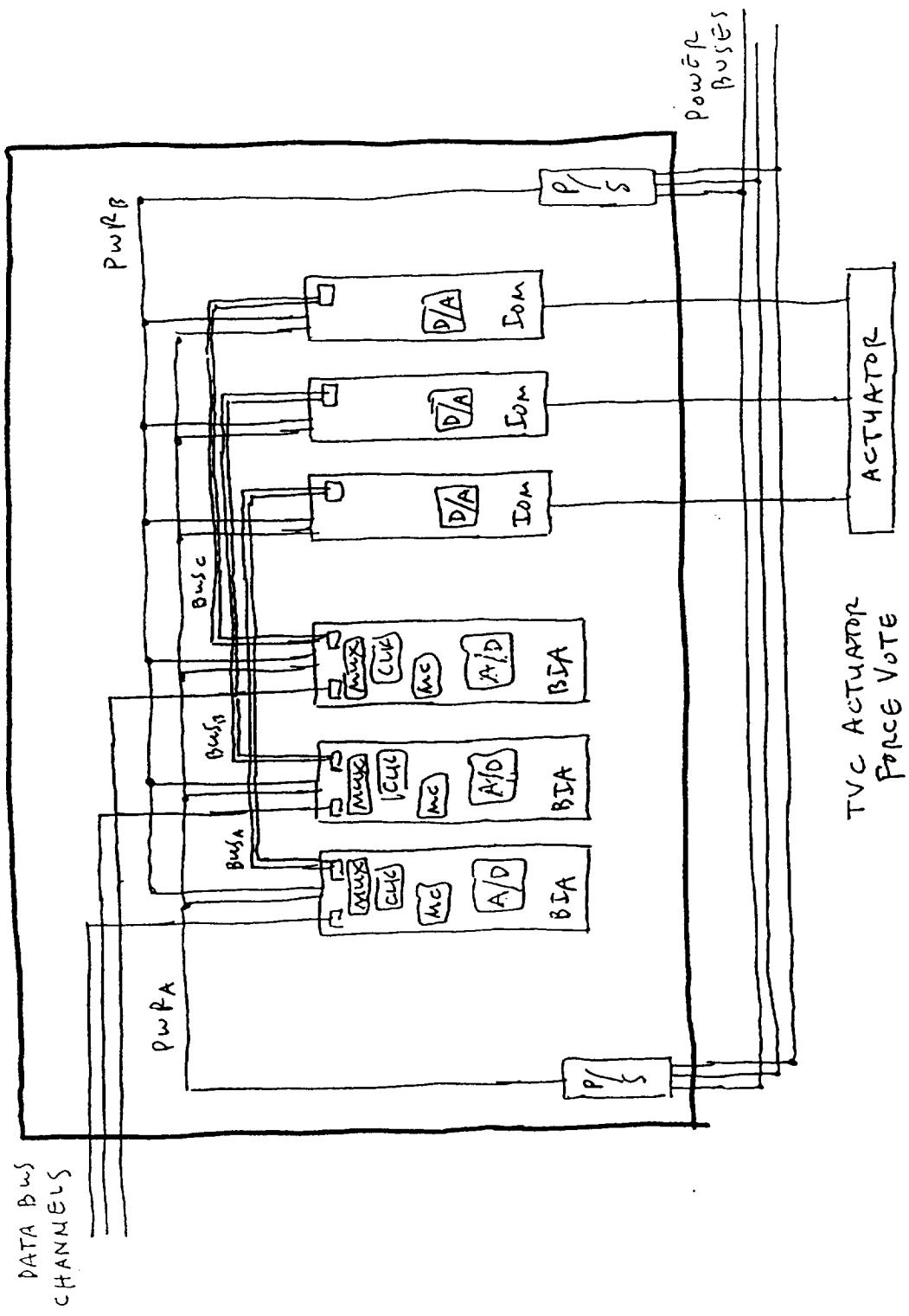
ACTUATOR FCRS (CHANNEL SWITCHOVER)



How Do You Avoid Failing in Here,
NEITHER CHANNEL IS DRIVING?

IO ANALYSIS

TMR REMOTE INTERFACE UNIT



P-O-P
REMOTE INTERFACE UNIT

